UNIVERSIDAD DEL SALVADOR

Facultad de Ciencias Económicas

Maestría en Auditoría de Sistemas

"La Necesidad de Implementar una Metodología para Conseguir un Nivel Óptimo de Seguridad y Protección de la Información para una Empresa"

TESIS

Previa a la obtención del título de:

MASTER EN AUDITORÍA DE SISTEMAS

Presentada por

Lady Maldonado

Tutor

Daniel Cazzasa

ARGENTINA - BUENOS AIRES

Año: 2010

RESUMEN

Este proyecto tiene como objetivo general, en base a la investigación realizada, elaborar una metodología de seguridad de la información, la cual pretende ayudar a una empresa a identificar y clasificar su información, detectar posibles riesgos y amenazas que atentan con la integridad, disponibilidad y confiabilidad de la información.

En el primer capítulo se describe una breve introducción acerca de la seguridad de la información, en la cual se menciona la evolución de las empresas frente a las nuevas tecnologías. Además se describe la justificación, objetivos y alcance del presente proyecto.

En el segundo capítulo se menciona la importancia para las empresas de mantener segura la información y no exponerla a riesgos y amenazas que atenten contra su operatoria. Además se detalla el valor y costo de la información para las empresas. Finalmente se presenta de manera resumida un estudio de delito digital, la cual ayuda al lector a conocer la problemática actual que viven las empresas en relación a seguridad de la información.

En el tercer capítulo se da a conocer los conceptos de seguridad de la información, riesgos, amenazas, vulnerabilidades y las diferentes medidas de seguridad a ser implementadas en las organizaciones. Adicionalmente se menciona la importancia de implementar una metodología de seguridad de la información.

En el cuarto capítulo se presenta de manera resumida las Normas y/o Estándares Internacionales vinculados a la seguridad de la información, a saber: COBIT, ISO 27001 e ISO 27002.

En el quinto capítulo se elaboró una metodología de seguridad de la información, la cual incorpora un marco de seguridad en torno a riesgos, amenazas y vulnerabilidades que enfrenta la información.

Finalmente se incluyen las conclusiones y anexos del presente proyecto de investigación.

ÍNDICE GENERAL

Pág.

RESUMEN.....I

ÍNDICE GENERAL.....II

ABREVIATURAS.....III

ÍNDICE DE GRÁFICOS.....IV

ÍNDICE DE TABLAS.....V

1. SEGURIDAD DE LA INFORMACIÓN.....1

1.1. Introducción.....1

1.2. Justificación.....2

1.3. Objetivos.....2

1.3.1 Objetivos generales.....3

1.3.2 Objetivos específicos.....3

1.4 Alcance.....4

2. ANTECEDENTES.....5

2.1. Evolución histórica de la seguridad.....5

2.2. Importancia de la seguridad de la información.....7

2.2.1. ¿Qué debemos proteger?.....9

2.2.2. Valor y costo de la información para las empresas.....10

2.3. Encuestas relacionadas con la seguridad de la información.....11

3. MARCO TEÓRICO.....16

3.1. ¿Qué es la seguridad de la información?.....16

3.1.1. Objetivos de la seguridad de la información.....17

3.2. Riesgo.....18

3.3. Amenazas.....19

3.3.1. Tipos de amenazas.....20

3.3.1.1. Amenazas humanas.....20

3.3.1.2. Maliciosas.....20

3.3.1.2.1. Externa.....20

3.3.1.2.2. Interna.....21

3.3.1.3. No maliciosas.....21

3.3.1.3.1. Externa.....21

3.3.1.3.2. Interna.....21
3.3.1.4. Amenazas por desastres naturales.....21
3.3.1.5. Otros.....22
3.4. Vulnerabilidades.....22
3.5. Relación Causa – Efecto.....24
3.6. ¿Cómo conseguir un nivel óptimo de seguridad y protección?.....24
3.6.1. Metodología de seguridad de la información.....24
3.6.1.1. Motivos para implementar una metodología.....25
3.6.2. Seguridad física.....26
3.6.2.1. Seguridad de acceso físico.....27
3.6.2.1.1. Organización.....27
3.6.2.1.1.1. Guardias de seguridad.....27
3.6.2.1.1.1.1. Detectores de metales.....28
3.6.2.1.1.2. Sistemas biométricos.....29
3.6.2.1.1.3. Protección electrónica.....29
3.6.2.1.2. Centro de procesamiento de datos.....29
3.6.2.2. Seguridad en la ubicación y dimensión del centro de procesamiento de datos.....31
3.6.2.2.1. Ubicación del área.....31
3.6.2.2.2. Dimensión de área.....32
3.6.2.3. Seguridad del equipamiento.....32
3.6.2.3.1. Aire acondicionado.....32
3.6.2.3.2. Instalación eléctrica y suministros de energía.....33
3.6.2.3.3. Temperatura y humedad.....36
3.6.2.3.4. Mantenimiento de los equipos.....36
3.6.2.3.5. Seguridad de los equipos fuera de las instalaciones.....37
3.6.2.3.6. Seguridad en la reutilización o eliminación de equipos.....38
3.6.2.4. Seguridad en contra de incendio y humo.....38
3.6.2.4.1. Incendios.....39
3.6.2.4.2. Humo.....41
3.6.2.5. Seguridad frente a desastres provocados por agua.....41
3.6.2.6. Seguridad de backups o respaldos.....42
3.6.2.6.1. Protección de respaldos.....43
3.6.2.7. Seguridad de otros equipos.....45
3.6.3. Seguridad lógica.....46
3.6.3.1. Seguridad en los accesos.....47
3.6.3.1.1. Identificación y autenticación.....47

3.6.3.1.1.1. Claves o passwords.....48
3.6.3.1.1.1.1. Pautas de elección de claves.....48
3.6.3.1.1.1.2. Reglas para proteger una clave.....50
3.6.3.1.1.1.3. Protección contra la intercepción de claves.....52
3.6.3.1.2. Roles.....52
3.6.3.1.3. Transacciones.....53
3.6.3.1.4. Modalidad de acceso.....53
3.6.3.1.5. Ubicación y horario.....54
3.6.3.1.6. Separación de las instalaciones de desarrollo, prueba y producción.....54
3.6.4. Seguridad en redes.....55
3.6.4.1. Seguridad en la red interna o intranet.....55
3.6.4.2. Seguridad en la red externa o extranet.....56
3.6.4.2.1. Peligros en la red externa.....56
3.6.4.2.2. Medidas de seguridad en Internet.....57
3.6.4.2.3. Firewall o puerta de seguridad.....57
3.6.4.2.3.1. Limitaciones del Firewall.....58
3.6.4.2.3.2. Antivirus.....59
3.6.5. Seguridad en los recursos humanos.....59
3.6.5.1. Investigación de antecedentes.....60
3.6.5.2. Acuerdos de confidencialidad.....61
3.6.5.3. Términos y condiciones en la relación laboral.....62
3.6.5.4. Capacitación continua y concientización.....62
3.6.5.5. Segregación de funciones.....63
3.6.5.6. Despidos y denuncias.....63
3.6.6. Seguridad en las contrataciones externas y outsourcing.....64
3.6.6.1. Riesgos del outsourcing.....64
3.6.6.2. Requisitos de seguridad en el outsourcing.....65
3.6.7. Plan de contingencias.....66
3.6.7.1. Contenido del plan de contingencias.....66
3.6.7.2. Etapas del plan de contingencia.....67

4. NORMAS Y/O ESTÁNDARES INTERNACIONALES.....69

4.1. COBIT (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas).....69
4.1.1. Usuarios.....69
4.1.2. Características de COBIT.....70

4.1.3. Principios de COBIT....70
4.1.4. Criterios de información....71
4.1.5. Recurso de TI....72
4.1.6. Orientado a procesos....73
4.1.7. Control....73
4.1.7.1. Controles de negocio y controles de TI....74
4.1.8. Controles generales de TI y controles de aplicación....74
4.2. ISO 27001....75
4.2.1. Sistema de gestión de seguridad de la información....76
4.2.2. Responsabilidad de la gerencia....77
4.2.3. Auditoría interna del SGSI....78
4.2.4. Revisión gerencial del SGSI....78
4.2.5. Mejoramiento del SGSI....79
4.3. ISO 27002 ex ISO 17799....79
4.3.1. Política de seguridad....80
4.3.2. Aspectos organizativos para la seguridad....81
4.3.3. Clasificación y control de activos....81
4.3.4. Seguridad del personal....82
4.3.5. Seguridad física y ambiental....82
4.3.6. Gestión de comunicaciones y operaciones....83
4.3.7. Control de accesos....83
4.3.8. Desarrollo y mantenimiento de sistemas....84
4.3.9. Administración de la continuidad de los negocios....84
4.3.10. Cumplimiento....85

5. METODOLOGÍA....86
5.1. Metodología de seguridad de la información....86
5.1.1. ASPECTOS ORGANIZATIVOS....86
5.1.1.1. Compromiso de la gerencia....86
5.1.1.2. Alcance....87
5.1.1.3. Política de seguridad de la información....88
5.1.1.3.1. Beneficios de implementar una política de seguridad....89
5.1.1.3.2. Elementos de un política de seguridad....90
5.1.2. ÁNALISIS DE RIESGO....91
5.1.2.1. Identificación de los activos de información....91
5.1.2.2. Propiedad de los activos de información....92

5.1.2.3. Clasificación de la información.....92
5.1.2.3.1. Clasificación del nivel de confidencialidad.....93
5.1.2.3.2. Tiempo de vida de la información.....94
5.1.2.4. Valoración del activo de información.....95
5.1.2.5. Clasificación de criticidad de los activos de información.....97
5.1.2.6. Nivel de riesgo de los activos de información.....98
5.1.2.7. Identificación de amenazas y vulnerabilidades.....98
5.1.2.7.1. Correlación de errores y ataques.....99
5.1.2.7.2. Amenazas y vulnerabilidades.....100
5.1.2.7.3. Valoración de las amenazas.....100
5.1.2.7.3.1. Análisis de impacto.....100
5.1.2.7.3.2. Análisis de probabilidad.....102
5.1.2.8. Determinación del nivel del riesgo.....102
5.1.3. TRATAMIENTO DE RIESGOS.....104
5.1.3.1. Tratamiento del riesgo.....104
5.1.3.2. Seleccionar e implantar controles de seguridad.....105
5.1.3.3. Riesgo residual.....107
5.1.4. IMPLEMENTACIÓN.....107
5.1.4.1. Implementación de la metodología.....107
5.1.5. MONITOREO.....108
5.1.5.1. Monitoreo de la metodología.....108
5.1.6. PROTECCIÓN DE LA INFORMACIÓN EN OTROS MEDIOS.....109
5.1.6.1. Información digital.....109
5.1.6.2. Información escrita e impresa.....110
5.1.6.3. Información "hablada".....110

6. CONCLUSIÓN.....112

ANEXOS

BIBLIOGRAFIA

GLOSARIO DE TÉRMINOS

ABREVIATURAS

TI	Tecnología Informática
COBIT	Control Objectives for Information and Related Technology
COSO	Committee of Sponsoring Organizations
ISO	International Standards Organization

ÍNDICE DE GRÁFICOS

Gráfico 2.1. Porcentaje de diferentes tipos de incidentes.....8

Gráfico 2.2. Principales tipos de incidentes de seguridad.....8

Gráfico 2.3. Principales fuentes de incidentes de seguridad.....9

Gráfico 2.4. Compañías que sufrieron incidentes.....12

Gráfico 2.5. Delitos Digitales más frecuentes en las organizaciones de negocios.....12

Gráfico 2.6. Pérdidas por Delitos Digitales.....13

Gráfico 2.7. ¿Se investigaron los Delitos Digitales ocurridos en la organización?.....13

Gráfico 2.8. Resultados para cada tipo de incidentes.....14

Gráfico 2.9. Denuncias ante las autoridades judiciales o policiales.....14

Gráfico 3.1. Tipos de Amenazas.....20

Gráfico 3.2. Relación causa-efecto.....24

Gráfico 4.1. Principios de COBIT.....71

Gráfico 4.2. Modelo PDCA aplicado a los proceso SGSI.....76

ÍNDICE DE TABLAS

Tabla 5.1. Activos de información y propietarios.....92

Tabla 5.2. Escala de Likert.....96

Tabla 5.3. Valoración de activos de información.....96

Tabla 5.4. Nivel de criticidad.....98

Tabla 5.5. Niveles de riesgo.....98

Tabla 5.6. Correlación de errores y ataques.....100

Tabla 5.7. Escala de estimación de la probabilidad de ocurrencia.....102

Tabla 5.8. Matriz de nivel de riesgos.....103

Tabla 5.9. Nivel del riesgo.....103

Tabla 5.10. Valoración de objetivos de control.....106

CAPÍTULO 1

1. SEGURIDAD DE LA INFORMACIÓN

1.1. Introducción

Desde la década de los 70 los sistemas de información, las nuevas tecnologías y la automatización en general han formado parte del desarrollo y la evolución de las empresas, en un principio se diseñaron aquellos sistemas y aplicaciones orientadas al mundo del negocio, sistematizando así los procesos de las empresas, logrando un avance importante que mejoraba la productividad, competitividad y desempeño.

Los avances tecnológicos han permitido el desarrollo de un sin número de industrias, y no sólo con equipos de alta tecnología que contribuyen al mejoramiento y la productividad en la prestación de servicios, sino que también han focalizado sus esfuerzos para construir verdaderos sistemas de información capaces del manejo y almacenamiento de gran cantidad de datos, logrando sistemas complejos para la toma de decisiones.

En el mundo globalizado de hoy, en el cual se integra todo lo referente a recursos de información como hardware, aplicaciones, sistemas, almacenamiento y recursos humanos; no podemos obviar un tema muy importante y que actualmente es de preocupación para todas las empresas, sean estas públicas o privadas; nos referimos a la SEGURIDAD DE LA INFORMACIÓN.

Es importante no olvidar la seguridad de la información, sobre todo porque los ejecutivos de cada empresa deben conocer que la información es el "activo más valioso de su organización" y se torna necesario mantener como objetivo constante la salvaguarda de dicho activo, administrando correctamente los riesgos e impactos del uso de tecnologías existentes y nuevas, estableciendo medidas de control que minimicen daños o pérdidas de información y ayuden a garantizar la operatividad y continuidad del entorno empresarial.

Por lo tanto uno de los objetivos de las organizaciones debería estar enfocado a establecer mecanismos que prevean la seguridad de su información, mediante una METODOLOGÍA DE SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN que contribuya en mantener la disponibilidad, integridad y confiabilidad de la misma.

1.2. Justificación

Entre los principales justificativos para implementar una metodología de seguridad y protección de la información encontramos los siguientes:

- √ Protección de la información frente a intrusos y visitantes no deseados que puedan atentar contra su disponibilidad, integridad y confidencialidad.

- √ Identificar los activos críticos de la empresa, determinando las vulnerabilidades existentes en lo relativo a controles de seguridad.

- √ Identificar los propietarios de los activos de información, junto con su grado de sensibilidad.

- √ Proteger la información con mayores riesgos y exposiciones existentes en el medio informático del negocio.

- √ Analizar los controles a implementar para mitigar los riesgos existentes.

- √ Evaluar la implementación de un sistema de gestión de riesgos.

- √ Fortalecer la organización a nivel de seguridad para lograr el avance y optimizar sus recursos.

1.3. Objetivos